I-DIN 9 RADIUS

I-DIN NINTH COMPANY LIMITED

i-DiN 9th
The ideas and innovation provider

What is RADIUS?

RADIUS, which stands for “Remote Authentication Dial In User Service”, is a network protocol - a system that defines rules and conventions for communication between network devices - for remote user authentication and accounting. Commonly used by Internet Service Providers (ISPs), cellular network providers, and corporate and educational networks, the RADIUS protocol serves three primary functions:

- Authenticates users or devices before allowing them access to a network
- Authorizes those users or devices for specific network services
- Accounts for and tracks the usage of those services

The RADIUS client server protocol contains many technological advantages for customers, including:

- An open and scalable solution
- Broad support by a large vendor base
- Easy modification
- Separation of security and communication processes
- Adaptable to most security systems
- Workable with any communication device that supports RADIUS client protocol

The RADIUS client-server architecture provides an open and scalable solution that is broadly supported by a large vendor base. It can be readily modified to meet a variety of situations. Customers can modify RADIUS-based authentication servers to work with a large number of security systems on the market. RADIUS servers work with any communications device that supports the RADIUS client protocol.

In addition, the flexibility of the RADIUS authentication mechanisms allows an organization to maintain any investment they may have made in an existing security technology: customers can modify the RADIUS server to run with any type of security technology. The flexible authentication mechanisms inherent in the RADIUS server facilitate its integration with existing and legacy systems when required.

Another advantage of the RADIUS architecture is that any component of a security system that supports the RADIUS protocols can derive authentication and authorization from the central RADIUS server. Alternatively, the central server can integrate with a separate authentication mechanism.

The utility of the RADIUS protocol extends beyond those systems that utilize network access devices and terminal servers for network access. RADIUS has been widely accepted by Internet Service Providers (ISPs) to provide Virtual Private Network (VPN) services. In this context, RADIUS technology allows an organi- zation to use ISP infrastructure for communications securely.

The distributive nature of RADIUS effectively separates the security processes (carried out on the authen- tication server) from the communications processes (implemented by the modem pool or the Network Access Server (NAS)), allowing for a single centralized information store for authorization and authenti- cation information. This centralization can significantly lessen the administrative burden of providing appropriate access control for a large number of remote users. If ensuring high availability is not a priority, then redundancy is not required; this centralization can thus be maximized, since all RADIUS-compatible hardware on a LAN can derive authentication services from a single server.

Features

More authentication types are supported by i-Din 9 RADIUS than by any other open source server. For example, i-Din 9 RADIUS is the only open source i-Din 9 RADIUS server to support Extensible Authentication Protocol (EAP).

i-Din 9 RADIUS is also the only open source i-Din 9 RADIUS server to support virtual servers. The use of virtual servers means that complex implementations are simplified and ongoing support and maintenance costs for network administrators are greatly reduced; thus, the ability of i-Din 9 RADIUS to support virtual servers gives it a huge advantage over the competition.

Modularity

The modular design protocol makes i-Din 9 RADIUS easy to understand. The modular interface also simplifies adding or removing modules - for example, if a feature is not needed for a particular configu- ration, the module is easily removed. Once the module is removed, it does not affect server performance, memory use, or security. This flexibility enables the server to run on platforms ranging from embedded systems to multi-core machines with gigabytes of RAM.

Scalability

A single RADIUS server can easily transition from handling one request every few seconds to handling thousands of requests per second, simply by reconfiguring a few default settings. Many large organi- zations (those with more than 10 million customers) are dependent on i-Din 9 RADIUS for their AAA needs. Often, only a single i-Din 9 RADIUS server is required to fill the needs of these large organizations.

While many commercial severs offer different versions of their software to handle different needs, only the latest version of i-Din 9 RADIUS is needed to obtain better performance, more realms, more RADIUS clients, and many other features, with no need to purchase additional product licenses

Customer Example - Structured Query Language (SQL)

Our client had designed a new network access system with custom query schema. Their user adminis- tration application was using the customer schema queries. When the client tested uninterrupted RADIUS protocol for scalability, they discovered that their RADIUS performance was one percent of the level they required. We were called in to help.

We determined that the table indices in their schema tables were not maximizing efficiently. So, we modified their table indices and updated the RADIUS configuration to use the new column as a key part of its queries.

The performance improvement was dramatic. The changes we made improved the client's system performance three hundredfold. Even better, the changes to the schema did not affect the client's user administration system.

Customer Example - AAA

Our client had used in-house expertise to create the authentication, authorization and accounting (AAA) policies for their organization. While their policies were correct, they began to experience performance problems as their user base grew. By working together, we found a solution.

By comparing their system requirements to the RADIUS server logs, we determined that the system was overloading the database storing their user information. When we examined the AAA policies they had written, the cause was clear.

To fix the problem, we re-wrote key portions of the clients' policies to add preconditions to the database queries. As a result, queries were done only when absolutely necessary. Reducing the number of access request queries was done without affecting any other policies on the system.

When we deployed the new policies, the load on their database dropped by a factor of four hundred. The decrease in load allowed the customer to keep their current systems and eliminated the need for an expensive hardware upgrade.

In addition to using their Network RADIUS SARL support contract to find solutions to problems, the customer was able to save money and optimize operations efficiency.

Customer Example - 802.1X

A customer wanted to deploy 802.1X authentication in his environment to enhance the security of his network. After weeks of effort, they had made no progress. We were called in to help and identified a number of problems.

The customer's networking equipment had a number of firmware issues. We worked with the vendor to fix those and additional issues that resulted from the firmware changes. Using the expertise gained from experience with other customers, we improved our customer's solution to prevent potential future problems.

We worked with an additional equipment vendor to identify undocumented product features to simplify the network configuration. We also tracked down and fixed interaction effects between our product and newer versions of Active Directory that had caused intermittent failures.

The end result was that the customer was able to deploy 802.1X authentication that met all of their requirements. A complex set of features were deployed across a wide range of networking equipment, supplied by a number of different vendors.

The additional network security was unobtrusive to network users. They could continue to use the network in their usual manner. The benefits of authenticating each user on the network were enormous to the network administrator.

Customer Example - Proxy

Our client’s legacy system used multiple RADIUS servers to proxy requests to different server destinations. Each RADIUS server implemented a set of policies, and was configured on all of the home servers. This duplication of information increased our customers network maintenance costs.

Upgrading to the i-Din 9 RADIUS product meant that the client could choose to continue to use multiple RADIUS servers, or replace them with one server, and update their configuration. If they chose to retain the multiple RADIUS servers, i-Din 9 RADIUS could re-use the common configuration. This re-use would lower their ongoing costs.

The client chose to replace the multiple RADIUS servers with a single server. The single server implemented all of their policies in walled garden sites that could not affect each other. The single server also performed all proxying to all home servers.

One result was that proxying became more robust. Instead of each server making fail-over decisions independently, the single server allowed information sharing across each walled garden. This resulted in faster fail-over when there was a problem, and faster fail-back when the home servers returned to service.

Fewer problems for users logging into the network meant increased customer satisfaction. The improved service and reduced maintenance costs also meant fewer support calls. With their end users happy, our customer was happy. Upgrading their legacy systems increased their revenue, and their profit.

Customer Example - Performance

Our customer had installed a basic RADIUS server with an SQL database back end. After a few months of operation, the system was performing at an unacceptable level.

We redesigned their system to allow the RADIUS servers to use the database more efficiently. We added tables, indices, and updated the RADIUS SQL queries. Our improvements helped our customer regain the system performance that they originally had. In addition, the performance gains were maintained even with ten times as much data in the SQL database as before.

Customer Example - Architecture

Our customer had installed a basic RADIUS server. They soon discovered that the performance did not meet their needs. The authentication process request for access response time was not sufficient. Our customer’s system accepted load was only a few authentications per second. On a high end machine, this was not acceptable.

We investigated, and determined that the problem was an external network dependency. The RADIUS server was waiting for another network element to respond before returning a response to the Network Access Server (NAS).

After optimizing their network configuration, their network achieved a rate of over 900 authentications per second. This performance level allowed them to move their new system into production.

How i-Din 9 RADIUS works

- AAA (Authorization, Authentication, and Accounting)
- RADIUS system components
- RADIUS session process
- RADIUS session messages

What is AAA?

AAA stands for “Authenication, Authorization, and Accounting”. It defines an architecture that authen- ticates and grants authorization to users and accounts for their activity. When AAA is not used, the architecture is described as "open", where anyone can gain access and do anything, without any tracking.

It is possible to incorporate only a portion of AAA in a system. For example, if a company is not concerned about billing users for their network usage, they may decide to both authenticate and authorize users, but ignore user activity and not bother with accounting. Similarly, a monitoring system will look for unusual user activity (accounting), but may cede the authentication and authorization decisions to another part of the network.

RADIUS is one of a number of Authentication, Authorization, and Accounting protocols. Other examples of AAA protocols include TACACS+ and Diameter.

Without AAA, a network administrator would have to statically configure a network. Even in the earliest days of dialup access, network administrators found a static model inadequate. AAA ensures the flexibility of network policies. AAA also gives network administrators the ability to move systems; without AAA, they would have to clearly define connectivity options.

Today, the proliferation of mobile devices, diverse network consumers, and varied network access methods combine to create an environment that places greater demands on AAA. AAA has a part to play in almost all the ways we access a network: wireless hotspots use AAA for security; partitioned networks require AAA to enforce access; all forms of remote access use AAA to authorize remote users.

AAA Definitions

The following sections describe each part of the AAA solution and how each one works.

Authentication

Authentication refers to the process of validating the identity of the user by matching the credentials supplied by the user (for example, name, password) to those configured on the AAA server (for example, name, password). If the credentials match, the user is authenticated and gains access to the network. If the credentials do not match, authentication fails, and network access is denied.

Authentication can also fail if user credentials are entered incorrectly. For example, site policy may allow a user network access from an on-site location using a cleartext password. However, if the same password is entered by the user from a remote location, access may be denied.

An ISP can also choose to deny network access to authenticated users if the users' account has been suspended. An administrator can choose to permit limited network access to unknown users, as well. For example, an administrator can provide access to an area where the user can purchase additional network connectivity. This last example is most often seen in for-pay WiFi hotspots.

Authorization

Authorization refers to the process of determining what permissions are granted to the user. For example, the user may or may not be permitted certain kinds of network access or allowed to issue certain commands.

The NAS sends a “request” - a packet of information about the user - and the RADIUS server either grants or denies authorization based solely on information in the “request” sent by the NAS.In each case, the RADIUS server manages the authorization policy and the NAS enforces the policy.

The NAS "request" is really a set of statements. For example, the NAS may send the RADIUS server a "request" containing the following user information:

"user name is Bob"

"password is Hello"

"ip address is 192.02.34"

Once the server receives the request, it uses that information to figure out what properties the user should have (i.e. "Bob" is saying he/she has IP address 192.0.2.34, do the server records contradict this statement?).

The server then sends a reply to the NAS. The reply contains a series of statements about what properties the user should have:

"user name is Bob"

"ip address is 192.0.2.78"

Note that the radius server can't request further information from the NAS. In contrast with SQL systems, RADIUS is limited in that it cannot make complicated queries. In SQL, queries such as "SELECT name from table where ip address = 192.02.34" are common. RADIUS does not have that capability. Instead, RADIUS only makes statements about what is, and what should be.

Upon receipt of a reply from the server, the NAS tries to enforce those properties on the user. If the properties cannot be enforced, the NAS closes the connection.

Authentication vs. Authorization

The following analogy illustrates the difference between Authentication and Authorization:

Imagine you are driving a car and you are stopped by a police officer. The officer asks you to provide a piece of identification to identify yourself. You could, for example, use your passport, driver’s license, or ID card to prove - or authenticate - who you are. In terms of the RADIUS protocol, the authentication process identifies the user as someone who is allowed to access the network.

The police officer may also ask you to prove that you are authorized to drive. In this case, there is only one document - a driver’s license - that proves that you are permitted - or authorized - to drive a car.

The authorization process thus combines the policy on the RADIUS server and the information in the request from the NAS. The NAS may add additional information to the request, such as the user’s Media Access Control (MAC) address. The NAS sends the information to the server, where an authorization decision is made.

Once the server processes this information, it sends a response to the NAS with instructions detailing which actions are allowed or denied. The NAS then monitors the user’s behavior and allows or denies activities according to the policy definition sent by the server.

Accounting

Accounting refers to the recording of resources a user consumes during the time they are on the network. The information gathered can include the amount of system time used, the amount of data sent, or the quantity of data received by the user during a session.

During a network session, the NAS periodically sends an accounting of user activity to the server. This accounting is a summary, rather than a complete copy of all traffic. This data is used for billing purposes.

ISPs are a large consumer of accounting data, because each user is billed for every minute of network access. However, corporations have not, historically, relied on network accounting information gathered by RADIUS because employees were not traditionally billed for network access. As their need for ongoing network monitoring increases, though, so does the need to store and process accounting information.

The accounting summary sent by the NAS to the server does not include detailed information such as web sites visited or even how many bytes were transferred using a particular protocol (SMTP, HTTP, and so forth). That type of detailed information is only available to the NAS, and it does not send that data to the server.

If detailed information about user activity is required, network administrators can obtain it through other protocols such as sFlow or NetFlow. However, those protocols are not integrated into RADIUS systems. Network administrators often find it difficult to tie the pieces together to get a more comprehensive understanding of user activity.

Auditing

Auditing refers to the proactive analysis of accounting logs and other data (such as sFlow or NetFlow data). This analysis is a long-term process and is part of ongoing maintenance and monitoring. Auditing provides information about the user’s post-authentication behavior. It can provide insight on when to update local site policy to best match user behavior.

Auditing can also be used to determine when an NAS has been compromised, by monitoring NAS enforcement of the required authorization policies. For example, if a user manages to override site policy and log into a particular server when the intent of the site policy was to deny that user access, an audit of the AAA records would highlight that policy violation. Since the intent of the site policy - to deny that user access - was overturned by the user, the audit would indicate that the site policy should be updated by the network administrator to prevent future policy violations. Subsequent audits would monitor long- term behavior and thus ensure that the policy is being enforced.

RADIUS System Components

RADIUS is a network protocol, a system that defines rules and conventions for communication between network device. Like many protocols, RADIUS uses a client-server model. A RADIUS client (also called a Network Access Server, or NAS) sends requests to a RADIUS server. The RADIUS server then processes the request and sends back a response.

Common NAS products include wireless access points such as the Linksys WRT54G and dial-up equipment commonly available from large network manufacturers. Common RADIUS server products include Cisco ACS, Microsoft IAS, Funk (now Juniper) Steel Belted RADIUS, Open Systems Radiator, and i-Din 9 RADIUS.

While the RADIUS protocol shares the general concept of client-server communication with many other protocols such as HTTP and SMTP, the specifics of RADIUS communications differ. This section describes the RADIUS system in more detail, including the specific roles of the NAS, the server, and databases such as MySQL and Lightweight Directory Access Protocol (LDAP).

See Table 2.1 for a list of RADIUS components and their descriptions.

RADIUS Components		
Component Name	Functions	Examples
User / Device	Requests access to the network.	Laptop Asymmetric Digital Subscriber Line (ADSL) Modem VOIP Phone
Network Access Server (NAS)	Provides access to the network for the user/device	Switch Wireless Access Point DSLAM VPN Terminator
Authentication Server	Receives authentication requests from the NAS. Returns authentication results to the NAS. Optionally requests user and configuration information from the database or directory. May return configuration parameters to the NAS. Receives accounting information from the NAS.	i-Din 9 RADIUS Radiator IAS NPS ACS
Data Store	Optional database or directory with user authentication and authorisation information. RADIUS server communicates with the data store using DB API or LDAP.	SQL Database Kerberos Service Server LDAP Directory

Network Access Server

The Network Access Server (NAS) acts as the gateway between the user and the wider network. When a user tries to obtain network access, the NAS passes authentication information (for example, user name and password) between the user and the RADIUS server. This process is termed an Authentication Session. Note that the user login initiates this Authentication Session conversation. This is a key concept.

At the end of the Authentication Session, the server instructs the NAS to either reject the user and deny network access or accept the user and provide network access. Once the user has accessed the network, security restrictions (defined by the RADIUS server) are enforced by the NAS, which acts as the gateway router and firewall for that user.

The RADIUS server receives a summary of the user's activities from the NAS. This summary includes data such as session identification information, total time on the network, and total traffic to and from the user. Note that user traffic does not pass through the RADIUS server - the RADIUS server only has access to user information via the NAS summary.

There are many different types of Network Access Servers (NAS). In an enterprise environment, network switches and wireless access points act as NASs to ensure only authorized users may access the corporate network. In contrast, carriers may use ADSL terminators or Digital Subscriber Line Access Multiplexers (DSLAM) as NASs to authenticate users and generate accounting information for billing. In fact, any device or application that verifies username and password authentication may be a RADIUS client.

RADIUS client NASs include FTP servers, web servers, and Unix login services.

Using the term server in reference to the Network Access Server can create confusion, because the NAS acts as a client in the RADIUS protocol. This document uses the term NAS to refer to a client and the term server to refer to a RADIUS Server.

RADIUS Server

The RADIUS server is usually a software application running on a Blade or self-contained server. RADIUS appliances with simplified maintenance and management interfaces are also available. In either case, the function of the server is identical: the server waits for a request from an NAS, processes or forwards the request, and then returns a response to the NAS. The response can contain authorization policies or an acknowledgment of accounting data received.

A single RADIUS server can receive and process many simultaneous access requests from numerous types of NASs (such as ADSL, dial-up, or VPN concentrators) in many different locations. A single server may also interact with flat files, SQL databases, LDAP directories, or other RADIUS servers. In order to make a decision regarding an access request, the RADIUS server must first use information from many sources.

Once the server makes a decision, it returns a response to the NAS. The NAS may enforce the policy in that response, or it may ignore it altogether. The server has no way of knowing if the NAS has received its response, or if the NAS is obeying the instructions in that response. Since it is customary for the NAS to log very little information about what has been received or how server responses are processed, it is very difficult to create and debug local site policies.

Consider the following analogy to help illustrate the point: a Human Resources (HR) department acts like a RADIUS server, by setting policies, and a security guard acts like the NAS in a network, by carrying out those HR department policies.

In this example, the company policy is that when an employee is fired, HR notifies security and removes building access from that employee. The security guard is then responsible for ensuring the fired employee no longer accesses the company building. If one day an employee gets fired (similar to a user being denied access) and the HR department informs the security guard (similar to the RADIUS server decision sent to the NAS), it is then up to the security guard at the company front desk to perform the task of refusing entry to the fired employee (similar to the NAS enforcing system access in a network). In the network, the NAS enforces system access. The RADIUS server does little more than offer advice to the NAS.

RADIUS Server Policies

The RADIUS server processes an NAS request based on the following criteria:

- Contents of the NAS request
- Information available locally to the RADUS server (flat files, SQL, LDAP)

The limitations inherent in the above processing criteria mean that the server cannot negotiate with an NAS to request more information: the server simply takes what the NAS sends and returns either an acknowledgment or a non-acknowledgment. This limitation is another key concept.

The RADIUS server has no control over the content of the request that the NAS sends.

Thus, once the RADIUS server receives the request from the NAS, it must use local information - policies or rules that a network administrator created and configured within the server - to decide how best to respond to the NAS request. The policies may be simple, such as “accept anyone with a correct user name and password”. Or, they may be complicated, such as “allow basic users to request premium services in non-premium hours, except for Sundays and holidays, so long as their payment status is up to date”.

In all cases, the policies must be designed, implemented, and deployed by the network administrator; this can be a significant effort, because policies are based on the contents of the NAS requests. Note that the NAS documentation does not always describe the content of the NAS requests; thus, in most cases, the only way for a network administrator to determine the NAS request content is to set up a test network. Test logins will result in the receipt of requests by the server. The administrator can then examine these requests to determine their content and create policies that look for those specific sets of attributes; once the policy is created, the server then uses that information to make decisions.

This process becomes more complicated when different NAS elements send the same information in different formats. For example, RADIUS has no MAC address data type, which means that the MAC address is sent as ASCII strings. Some NAS elements send a MAC address in the format of “00:01:02:03:04:05”, while others use the format “00-01-02-03-04-05”. The fact that these differences are not documented makes policy creation very difficult.In most cases, the administrator has to resort to trial and error methods to determine how to implement policies.

Data Stores

Data stores (i.e., databases or directories) permit the storage and retrieval of data. They have limited decision-making capabilities. While stored procedures are possible in most databases, they are rarely used when simple data storage is required.

The key differences between RADIUS servers and data stores are the way they support policies and authentication. The role of a data store in the authentication process is to provide data to a RADIUS server. The server then uses an authentication method to authenticate the user.

When a RADIUS server authenticates a user or stores accounting data for that user, it reads from or writes to a database or directory.User information (i.e., user name, password, credit amount) and session data (i.e., total session time and statistics for total traffic to and from the user) are stored on this database or directory.

In many respects, the RADIUS protocol is similar to a remote database query language. Specifically, while an SQL or LDAP database stores user data, that database cannot be queried directly by the NAS. Instead, the NAS sends a request to the server, which in turn queries the database. This simplification of the normal database query language means that it is easy to add authentication and accounting to an NAS instead of implementing a full-featured SQL client, which would be very resource intensive and costly.

Key Differences Between RADIUS Servers and Data Stores	
RADIUS Servers	Data Stores
Implement policies	Rarely implement policies
Support complete authentication protocols sets, such as: ● CHAP ● MS-CHAP ● MS-CHAPv2 ● 802.1X (EAP, EAP-TLS, PEAP, EAP-TTLS, EAP-MD5, EAP-GTC, LEAP) ● HTTP Digest authentication	Permit simple authentication queries, such as: ● LDAP “bind as user”

RADIUS System Components Summary

In summary:

- An NAS is responsible for requesting and enforcing network access, filtering traffic, and sending summaries of accounting data.
- The RADIUS server is responsible for receiving access requests, interpreting complex policies, and returning a response to the NAS.
- A data store (i.e., directory or database) is responsible for storing large amounts of data, most often keyed by user name. This data may include user passwords, credit amounts, session data, and more.

The RADIUS Session Process

A RADIUS session consists of the following steps:

1. A remote user connects to a RADIUS client device (using Point-to-Point Protocol (PPP, 802.1X) or another Data Layer link protocol) and initiates a login:
    - The NAS initiates all conversations (Authentication Sessions) in RADIUS.
    - All information sent to the server is done solely at the discretion of the client.
    - The RADIUS server does not control what the NAS sends.

2. The Network Access Server communicates with the RADIUS server using a shared secret mechanism:
   - RADIUS uses User Datagram Protocol (UDP) port 1812 for authentication and 1813 for accounting.

3. The NAS sends a RADIUS message (called an Access-Request) to the server.
   - This message contains information about the user, including user name, authentication creden-tials, and requested service.
   - In addition, the message may contain information about the NAS, such as its host name, MAC address, or wireless SSID.
   - The message is sent using the Password Authentication Protocol (PAP), Challenge-Handshake Authentication Protocol (CHAP), or Extensible Authentication Protocol (EAP).
   - The server must decide whether to authenticate or authorize a user based solely on the informa- tion contained within the NAS request, as it does not have access to any additional user informa- tion.
   - If the NAS sends a packet with an authentication protocol that the server does not support, the server will reject that request.

4. The RADIUS server processes the request and verifies the login request against either a local data-base or the authentication service running on the network.
   - Authentication services can include: LDAP servers for a domain validation; Active Directory servers on Windows networks; Kerberos servers; SQL Server or another type of database for getting information from a database

5. The RADIUS server sends validation results back to the NAS in one of the following forms: Access Reject, Access Challenge, or Access Accept.
    - Access Reject locks the user out of the network if the user is invalid or not authorized, denying them access to the requested resource.
    - Access Challenge occurs when the server requires additional information from the user. Since RADIUS packages are limited in size, Access Challenges allow the exchange of larger amounts of data.
    - Access Accept provides the user access to the resource and contains policy information which the NAS uses to provide services to, and enforce the behavior of the user. An Access Accept condition does not apply to all resources. Each additional resource is checked as required. The RADIUS client also verifies the original access offered on a periodic basis.
    - An Access Accept response results in the NAS providing the following services to the remote client: supplying a static or dynamic IP address; assigning a Time-to-Live for the session; downloading and applying the users' Access Control List (ACL); setting up any L2TP, VLAN, and QoS session parameters required

6. Once the session is established on the RADIUS client, the accounting process is initiated:
    - The *Accounting-Request (start)* message, sent by the NAS to the server, indicates the commencement of the session. The the session account record is then created.
    - The *Accounting-Request (stop)* message indicates the end of the session; the session account record is then closed.

- The data stored in the database during the accounting sessions is used to generate billable infor-mation and reports.
- Accounting information retained in the database includes the following: time of session, number of packets and amount of data transferred, user and machine identification, network address, and point of attachment information.

RADIUS Session Messages

A RADIUS session message consists of a single User Datagram Protocol (UDP) packet, containing a short header followed by the authentication, authorization, or accounting data.

Message Attributes

Each message contains a list of Attribute Value Pairs (AVPs), commonly referred to as attributes. These attributes carry information from the NAS to the server or virtual proxy server and from the server to the NAS. Common attributes include items such as user name, password, IP address, and NAS address; each attribute contains only one of these items. An attribute can also contain sub-attributes, for grouping purposes.

Each client and server supports only a limited set of attributes. In some cases, attributes may not be supported because the server or NAS software may have been written before a standard was published, or the software may simply not support that particular functionality. The best way to know which attributes are supported is to consult the software vendor documentation. If the documentation is silent on the topic, the attributes in question are probably not supported. Contact the vendor for additional information.

In addition to standardized attributes, vendors can extend RADIUS with vendor-specific attributes (VSAs). Using VSAs means that the vendor can rapidly add functionality without having to do a time-consuming standardization process.

In order to be useful in the RADIUS client protocol, however, VSAs must be defined on the RADIUS server. Because VSAs are non-standardized attributes, it is difficult to discover any information about them. In addition, they are all vendor-specific (only work on that vendor's products). Thus, defining VSAs for RADIUS server use may be difficult.